Understanding the "Organizational" Dimension of Health Information Security

Jeff Collmann, PhD
Imaging Science and Information Systems Research Center, Department of Radiology, Georgetown University Medical Center
collmann@isis.imac.georgetown.edu

When the National Library of Medicine (NLM) issued its request for proposals for applications of the national information infrastructure to health care, it required that all projects examine the technical and organizational dimensions of computer-based health data security. As a result of Project Phoenix, an NLM-supported telemedicine network supporting hemodialysis in patients with end-stage renal disease, we came to understand "the organizational dimension" of data security as the result of the complex interaction of three facets: (1) data-security-related activities, (2)organizational functions supporting data security, and (3) organizational conditions that sustain or undermine data security. By activities, we mean all those tasks and programs that organizations accomplish in the name of improving the security of health information, such as assessing risk, auditing logbooks, sponsoring training, and investigating security incidents. Organizations frequently sponsor activities while discharging broad functions that support data security. We have defined three data security functions as particularly important: (1) monitoring changing regulations, laws, and professional standards; (2) continuously reviewing, revising, and enforcing data security policies, procedures, and practices; and (3) enhancing patient understanding of an organization's data security program. Sustaining such security-related activities and functions, however, requires organizations to bridge social boundaries that tend to reduce communication and collaboration about data security among their constituent units. We have identified three important methods organizations can use to bridge boundaries: (1) sponsoring interdisciplinary, interdepartmental work groups, (2) establishing formal partnerships among the people and units responsible for all aspects of information management, and (3) encouraging informal communities of proponents who support sound data security practices while discharging their regular responsibilities. This paper illustrates these points with examples from Project Phoenix, the U.S. Department of Defense, and Kaiser Permanente.

ACKNOWLEDGMENTS

This project has been funded in whole or in part with Federal funds from NLM under Contract No. N01-LM-6-3544 and an Interagency Personnel Agreement between Georgetown University Medical Center and the Telemedicine and Advanced Technology Research Center, U.S. Army Medical Research and Materiel Command, Ft. Detrick, MD.